Optometry Coding & Billing Alert

HIPAA: Solidify Your HIPAA Policies and Practices Before the Auditors Come Knocking

All covered entities and business associates are on the audit list, HHS says.

HIPAA is a core component of every practices day-to-day policies, but if you aren't following your practice's policies and procedures, your practice may face penalties. Is your practice prepared for a HIPAA audit?

The Health Information Technology for Economic and Clinical Health Act (HITECH) §13411 now requires the U.S. Department of Health and Human Services (HHS) to periodically audit covered entities and business associates subject to HIPAA Privacy and Security rules, according to Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, Ver. HHS is redesigning the random audit program, with new audits to be performed by HHS staff starting Oct. 1, 2013 □ just eight days after the new rules are enforceable.

Get ready: "Everyone is an audit target, all covered entities and all business associates," warned Susan A. Miller, JD in an issue brief for Malvern, Penn.-based Malvern Group Incorporated. The HHS Office for Civil Rights (OCR) "is going to be knocking on everyone's digital door in the near future. It appears that OCR will audit all covered entities and business associates periodically."

Get Ready Now □ What to Expect

A HIPAA audit basically aims to determine whether you have in place all the HIPAA-required policies and procedures, Sheldon-Dean explains. You also have to show that you've been using these policies and procedures.

And you'll need to offer up a mountain of documentation that auditors will ask for □ everything from your training policies, materials and rosters to your security incident policy and security incident reports, Sheldon-Dean says. Worst of all, you'll have just three weeks' notice to produce this substantial documentation and prepare for the on-site audit.

Beware: Auditors can and will interview staff members □ any staff they choose, Sheldon-Dean cautions. "You must be prepared in advance or it's too late."

Pay attention: And the audits will be more specific and focus on particular problem areas. Sheldon-Dean predicts that auditors will scrutinize the following areas the most:

- Whether you have an updated Notice of Privacy Practices (NPP);
- Compliance with the new privacy rights and restrictions.

Know the New Enforcement Definitions

The HIPAA Omnibus final rule introduced and solidified a new penalty structure, as well as new definitions relating to HIPAA violations. The definitions for three terms in particular are rather pivotal under the new, tougher penalty structure.

- Reasonable Cause: An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.
- Reasonable Diligence: Business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- Willful Neglect: Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

What's more: Willful neglect violations must be investigated and penalties are mandatory, Sheldon-Dean points out. And the HITECH provisions allow continued corrective actions, even if there's no penalty. Plus, now your state Attorney General can bring HIPAA actions.

How Wrongful Disclosures Apply to Individuals Too

Under HITECH §13409 (Wrongful Disclosures), such violations can apply to individuals and are now being used in criminal cases, Sheldon-Dean says. Further, civil lawsuits involving HIPAA violations are becoming increasingly common and with escalating verdict awards.

Case in point: A July 26, 2013 jury verdict from the Indiana Superior Court awarded a Walgreens pharmacy customer $1.44 million after her pharmacist leaked her PHI to other individuals who allegedly used that customer's PHI to intimidate and harass her. The customer filed a lawsuit against not only Walgreens, but also the pharmacist as an individual.

This case illustrates the newest legal evolution in HIPAA violations although not the first case in which HIPAA has been involved in a private cause of action, it is "the first case resulting in a substantial jury verdict against a provider using HIPAA as the basis for the standard of care," according to a recent legal analysis in an article by Theodore J. Kobus III and Lynn Sessions of Cleveland, Ohio-based law firm Baker Hostetler.

"Whether and to what extent HIPAA can be used to establish the standard of care in a professional liability, negligence or other breach of professional duty case will be dependent on state tort law," the attorneys wrote. "Healthcare providers must be aware that, depending on the law of the state in which they are licensed, their potential liability for HIPAA violations could extend beyond civil monetary penalties."

Understand the New Tiered Penalty Structure

Also, you're now facing higher penalties for HIPAA violations, effective for incidents after Feb. 17, 2009. The new maximum penalty is $1.5 million for all violations of a similar type in one calendar year. Sheldon-Dean breaks down the new penalty tiers:

- Tier 1: Did not know and, with reasonable diligence, would not have known $100 to $50,000 per violation.
- Tier 2: Violation due to reasonable cause and not willful neglect $1,000 to $50,000 per violation.
- Tier 3: Violation due to willful neglect and corrected within 30 days of when known or should have been known with reasonable diligence $10,000 to $50,000 per violation.
- Tier 4: Violation due to willful neglect and not corrected within 30 days of when known or should have been known with reasonable diligence $50,000 per violation.